Atelier SI-F – AFNOG 2008

Bases Internet Protocol

Alex Corenthin
corenthin@ucad.sn

Présentation générale

- TCP/IP = suite de protocoles "réseau"
  - Protocoles publics
  - Adressage logique
  - Protocole "routable"
  - Service de "nommage"
  - Contrôle des erreurs et flots de données
  - Support applicatif (ports)

Organisation

TCP/IP = protocole ouvert, public

ISOC (Internet Society)
- IAB (Internet Architecture Board)
  Gestion et fonctionnement d'internet
- IETF (Internet Engineering Task Force)
  Spécifications techniques d'internet
- IANA – Autorité d'Assignation de ressources Internet
- IRTF (Internet Research Task Force)
  Recherches autour de TCP/IP

RFC : Request For Comments

Modèle OSI

APPLICATION
- couches supérieures
- Orientées applications
- Indépendance vis à vis des couches basses

TRANSPORT
- Couches basses
- Transmission des données
- No differentiation of upper layers

Couche Physique: "Accès au réseau"

- Accès au réseau physique
- Envoyer et recevoir des datagrames IP

•Interface avec la carte réseau
•Coordination de la transmission des données
•Formatage des données
•Conversion des signaux analogiques/numériques
•Contrôle d'erreurs des trames
(ajout d'infos, contrôle à l'arrivée, accusés de réception,..)

Ethernet, Token Ring, FDDI, SLIP, PPP,…

Couche Liaison:
Transmission sans erreur de codage

- Transmission sans erreur des datagrammes entre 2 systèmes adjacents.
- Masque aux couches supérieurs les imperfections du moyen de transmission.
- Moyen: codage redondant (parité, …)
- Le protocole de correction n'est pas forcément le même entre deux nœuds adjacents.

Couche réseau:
crée la « base » du réseau.

- C'est la « couche IP ».
- Permet à 2 systèmes non-adjacents de communiquer en se servant de relais.
- Notion d'@ est importante.
- Notion de table de correspondance entre @ et fils pour aiguiller les messages.
- **Routage**:

Couche transport:
Délivrer un message complet entre deux machines non-adjacentes.

- C'est la « couche UDP/TCP »
- Permet d'offrir un service constant, quelque soit les qualités du réseau utilisé.
- Permet de gérer la perte d'un paquet
- Réorganise les paquets à l'arrivée.

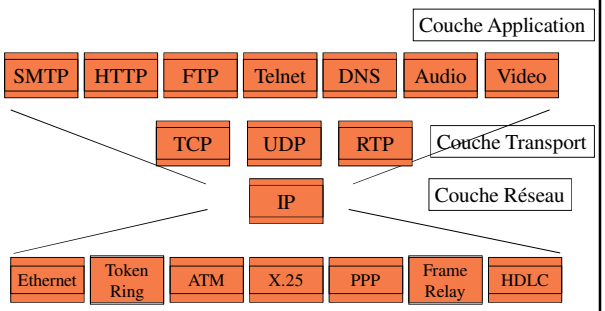
Couches supérieures: Session, présentation et application

- La couche session permet d'établir une relation durable entre deux applications souhaitant coopérer (visio conférence…) (*pas obligatoire*)
- La couche présentation permet de résoudre les problèmes de codage des données hétérogènes (big/little endians).
- La couche application fournit les services de communication aux utilisateurs (mail, transfert de fichier, …)

OSI et TCP/IP

		TCP/IP	
7	Application	Application	*Mail, Web, etc.*
6	Presentation		
5	Session		
4	Transport	Transport	*TCP/UDP – end to end reliability*
3	Network	Network	*IP - Forwarding (best-effort)*
2	Data Link	Data Link &	*Framing, delivery*
1	Physical	Physical	*Raw signal*

Couches de protocoles : Le modèle TCP/IP

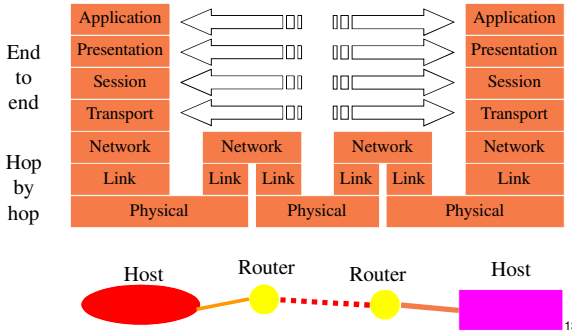


Interactions entre couches

- Les couches Application, Presentation and Session et les protocoles associés sont en mode bout-à-bout (end-to-end)
- Le protocole de Transport est end-to-end
  - encapsulation/décapsulation à travers le protocole réseau sur les systèmes terminaux
- Le protocole de réseau effectue l'interconnexion des réseaux physiques
  - encapsulation/décapsulation au dessus de la couche de données à chaque noeud

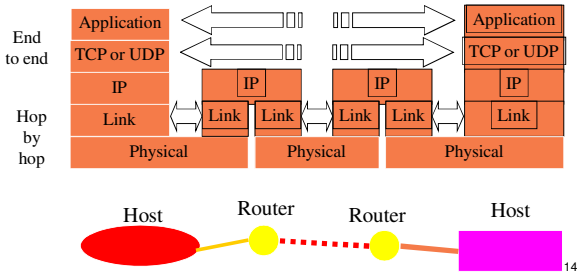
  Les couches liaisons et physiques peuvent être différentes à chaque noeud

Interaction entre couches: Modèle OSI à 7 couches

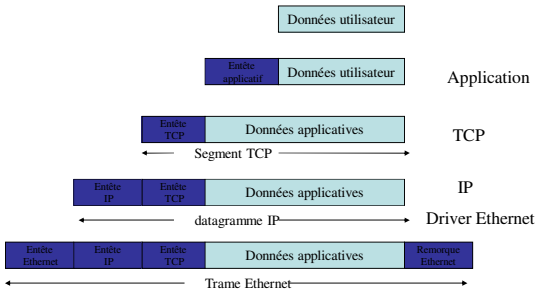


Interactions entre couches : Modèle TCP/IP

Pas de couches session et presentation dans le modèle TCP/IP



Encapsulation / Décapsulation



Trame, Datagramme, Segment, Paquet

- Ce sont les différents noms des paquets à différents niveaux
- Trame Ethernet (couche liaison)
  - Datagramme IP (couche réseau)
  - Segment TCP (couche transport)
- La Terminologie n'est pas respectée
  - On utilise le terme "paquet" à tous les niveaux

Couche 2 – Trame Ethernet

Preamble	Dest	Source	Length	Type	Data	CRC
	6 bytes	6 bytes	2 bytes	2 bytes	46 to 1500 bytes	4 bytes

- Adresses destination et source sont au format 48-bit (addresses MAC)
- Type = 0x0800 signifie que le champ donnéesde la trame Ethernet contient un datagramme IP. Type = 0x0806 pour ARP.

Couche 3 – Datagramme IP

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source Address				
Destination Address				
Options				Padding
Data				

- Version = 4
- If no options, IHL = 5
- Adresses Source et Destination au format 32-bit IP

Champ Protocol = 6 signifie que le champ “data” contient un segment TCP.

Champ Protocol = 17 : segment UDP.

Couche 4 - TCP segment

Source Port								Destination Port
Sequence Number								
Acknowledgement Number								
Data Offset	Reserved	U R G	A C K	E O L	R S T	S Y N	F I N	Window
Checksum								Urgent Pointer
Options								Padding
Data								

Les champs Source and Destination sont au format 16-bit (numéros de ports TCP, les addresses IP sont gérées par l'en tête IP)

Sans options, Data Offset = 5 (which means 20 octets)

Caractéristiques principales des Réseaux

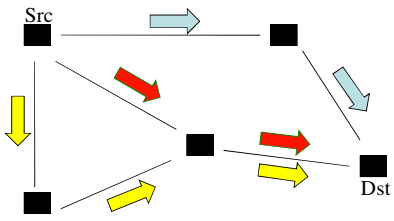
Caractérisation par :

- Type des connexions
  point à point / multipoint
- Topologie
  maillage / bus / anneau / étoile / arbre ...
- Taille du réseau
  LAN / MAN / WAN / internet

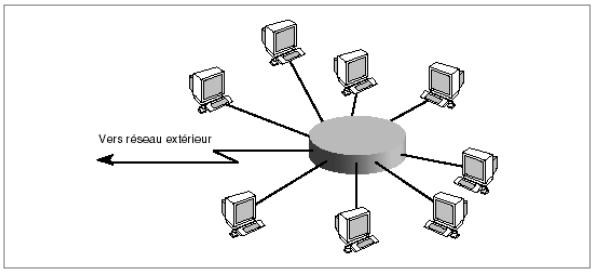
Point à Point / Multipoint

- Liaison (connexion) point à point
  - un canal est dédié spécifiquement à la connexion de deux machines
- Réseau point à point
  - ensemble de liaisons point à point
- Liaison (réseau) multipoint
  - Un canal est partagé par un ensemble de machines

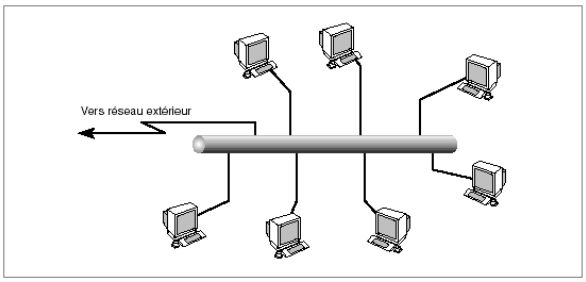
Réseau point à point (Maillage) Problème du routage



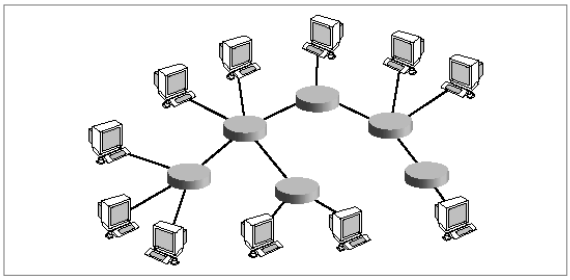
Topologie en étoile



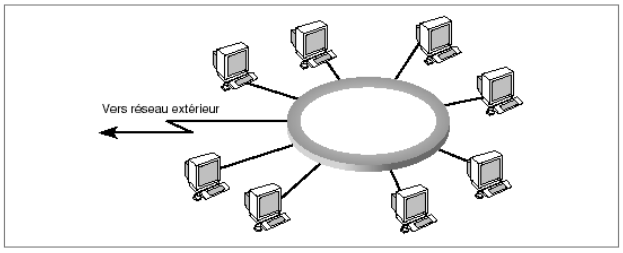
Topologie en bus



Topologie en arbre

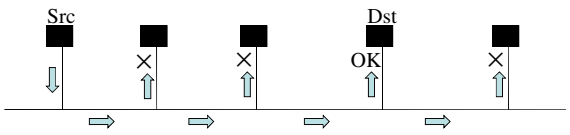


Topologie en anneau



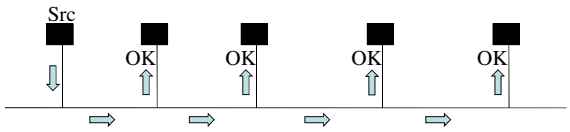
Communication Unicast

- Une machine (source) envoie un message à une machine destination



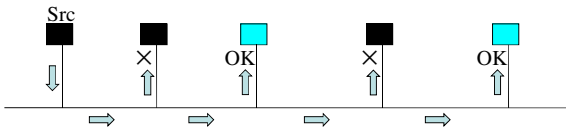
Communication Broadcast

- Diffusion générale : une machine (source) envoie un message à toutes les machines



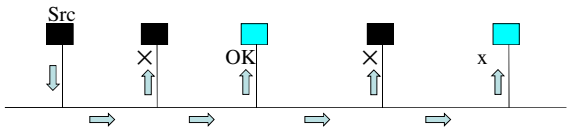
Communication Multicast

- Diffusion restreinte : une machine envoie un message aux machines d'un groupe



Communication Anycast

- Une machine (source) envoie un message à une machine destination, délivré à la machine la plus **topologiquement** proche



IP : Internet Protocol

- But: Acheminement des datagrames d'une machine à une autre par des intermédiaires .
  - Adressage logique, indépendant du matériel (distribution supervisée des adresses)
  - Routage (comment ces adresses sont elles traitées?)
  - Correspondance entre adresse physique et adresse logique (DNS et DHCP)

IP Internet Protocol (2)

- Le protocole IP définit :
  - La taille de l'unité de donnée, sa structure.
  - La fonction de routage, comment les machines et les passerelles doivent traiter les paquets.
  - Les messages d'erreur et leurs traitement.
- L'entête IP contient
  - Version, longueur, priorité, durée de vie, @ source et @ destination.
  - Options de routage, de traçage, …

Adressage IP

- Système de communication universel : établir une méthode générale d'identification des machines.
  Coexistence de 2 versions IPv4 et IPv6

  en version 4.

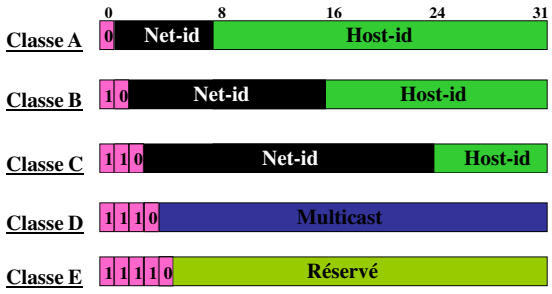
➢ 32 bits utilisés, écriture en 4 fois 8 bits.
  11000000 10101000 00001020 10000010 = 192 168 10 130

- Adresse = 32 bits = 4 octets = 4 entiers < 256
- Adresse est en 2 parties :
  - Net ID : Identifiant du réseau
  - Host ID : Identifiant de la "machine"

Adressage IPv4

- **Une adresse IP :**
  - 4 octets (32 bits),
  - notation « décimal pointé » A.B.C.D.
  - exemples : 130.190.5.1 193.32.20.150 134.157.4.14
- **Elle doit être unique au Monde**
  - configurable par logiciel
  - associée à chaque interface réseau
- **Attribution des adresses de réseau en Afrique:**
  - RIR (Regional Internet Registry)
    - AfriNIC (Network Information Center) de l'Internet pour l'Afrique
    - mail à hostmaster@afrinic.net
  - LIR - Local Internet registries dans les pays :
    - Généralement Opérateurs d'accès à Internet
    - Opérateurs historiques des télécommunications

Adressage IPv4 : 5 Classes d'adresses (Ancien modèle)



L'adressage IP

L'adressage d'une machine/d'un réseau
=
@ IP + masque sous-réseau (exception avec la notion de *classes*).

1 réseau IP = 1 plage IP constituée par :

- ✓d'une adresse définissant le réseau (première adresse de la plage).
- ✓d'une adresse définissant le broadcast réseau (la dernière adresse de la plage).
- ✓d'adresses des hôtes uniques (toutes les autres adresses).

Il existe des exceptions : des plages IP réservées et d'autres à ne pas router.

Adressage IPv4 : Adresses réservées (RFC 3330)

- Host-Id = 00000…000 -> Réseau
- Host-Id = 11111…111 -> Broadcast

- 127.x.x.x ->loopback
- 10.0.0.0 à 10.255.255.255 -> privé
- 172.16.0.0 à 172.31.255.255 -> privé
- 192.168.0.0 à 192.168.255.255 -> privé

ARP

Rappels - Ethernet

- Ethernet fonctionne en mode Broadcast
- Structure de la Trame Ethernet :

Preamble	Dest	Source	Length	Type	Data	CRC

- Le paquet IP packet est contenu dans le champ données de la trame Ethernet
- Algorithme de transfert (CSMA/CD)

Ethernet/IP Address Resolution

- Adresses Internet
  - Unicité worldwide (sauf réseaux privés)
  - Indépendantes du réseau Physique
- Adresses Ethernet
  - Unicité suivant la norme (sauf erreurs)
  - Ethernet Only
- Nécessité de correspondance entre couches hautes et basses
  - *(IP vers Ethernet, en utilisant ARP)*

Address Resolution Protocol

1. Consultation du Cache ARP cache pour rechercher la correspondance avec l'adresse IP
2. Si elle n'est pas présente, broadcast un paquet contenant l'adresse IP recherchée à toutes les machines sur Ethernet
- "propriétaire" de l'adresse IP répond
1. La reponse est stockée dans la table ARP pour une utilisation future
2. Les entrées obsolètes sont retirées après un certain temps (notion de timeout)

Procédure ARP (requête)

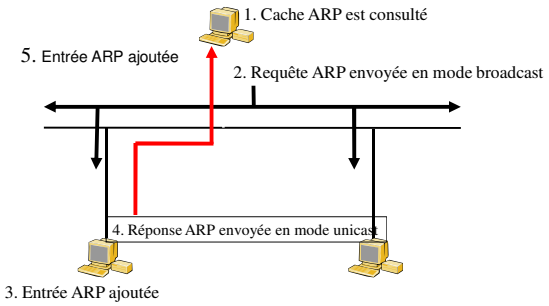


Table ARP

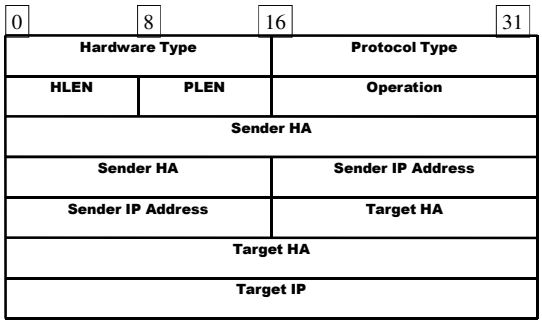
IP Address	Hardware Address	Age (Sec)
192.168.0.2	08-00-20-08-70-54	3
192.168.0.65	05-02-20-08-88-33	120
192.168.0.34	07-01-20-08-73-22	43

Trame ARP

- message ARP est encapsulé dans une trame Ethernet

Dest Addr	Source Addr	Frame Type	Frame Data
		0x806	Arp Message

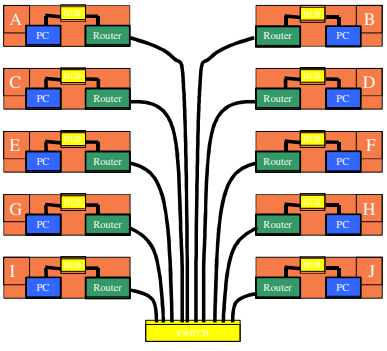
Format du message ARP



Types of ARP Messages

- ARP request
  - Who is IP addr X.X.X.X tell IP addr Y.Y.Y.Y
- ARP reply
  - IP addr X.X.X.X is Ethernet Address hh:hh:hh:hh:hh:hh

Exercice Addressage IPv4



Exercice Addressage IPv4

- Déterminer l'adresse IP pour la connection de votre routeur de connection au réseau d'interconnection.
- 196.200.221.64+X
  - x = 1 pour la table 1, 2 table 2, etc.
  - Ecrire cette adresse dans sa forme décimale, binaire et Hexadécimale.

Sous réseaux : Subneting

Pourquoi *fragmenter* un réseau ?

- Optimisation des tables de routage
  - Connaître @ rezo pour envoyer dans une direction générale
  - Ce n'est qu'une fois arrivé près de la machine que l'on résout son adresse.
  - Métaphore du colis de la Poste. (Code postal: département, centre de tri, puis : rue, numéro, nom)
- Limiter les congestions.
- Séparer les machines sensibles.

Sous réseaux : Principe

- C'est un séparateur entre la partie réseau et la partie machine d'une @ IP.
- Une fonction ET Logique pour déterminer l'@ réseau.
- Il est recommandé d'avoir des bits à 1 contiguës dans ses masques.

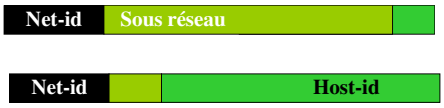
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0

Masque de sous réseau

Sous réseau : Principe (2)

- Mon adresse IP: 192.168.25.132
  Traduit en binaire:
  11000000.10101000.00011001.10000100
- Le masque de mon réseau: 255.255.255.128
  Traduit en binaire:
  11111111.11111111.11111111.10000000
- @ réseau:
  11000000.10101000.00011001.10000000
  Soit: 192.168.25.128
- **Conclusion: on peut supposer que les machines de mon réseau local ont pour adresse: 128 à 254…**

Sous réseaux : Les choix



Le choix se fait en fonction des besoins et des limites:
- Une plage est allouée par le fournisseur d'accès.
- Un nombre de machines qui peut croître.

L'adressage **CIDR**
Classless Inter Domain Routing

Le masque sous-réseau permet de créer des sous-réseaux ou sur-réseaux qui ne respectent plus le découpage en classes A, B, C.

C'est le masque de sous-réseau qui définit la limite des bits d'adressage du réseau, des bits d'adressage de la machine :

192.168.10.5/255.255.255.0 ou 192.168.10.5/24 ← 24 bits Rx sur 32
→ 192.168.10.0 → 192.168.10.255

192.168.10.5/255.255.255.128 ou 192.168.10.5/25 ← 25 bits Rx sur 32
→ 192.168.10.0 → 192.168.10.127

192.168.10.5/255.255.252.0 ou 192.168.10.5/22 ← 22 bits Rx sur 32
→ 192.168.8.0 → 192.168.11.0

Exercices:

- Soit le réseau d'@ 192.168.25.32
  de masque 255.255.255.248
  La machine 192.168.25.47 appartient-elle à ce réseau?
- Soit le réseau d'@ 193.225.34.0
  de masque 255.255.255.0
  Nous voulons installer 60 machines…
  Quel masque utiliser?

IPv6

- Adressage

Adressage IPv6 : Les motivations

- Croissance exponentielle de la taille d'Internet
  - Épuisement des adresses Ipv4 (Ipv4 exhaution → 2011 ??)
  - Explosion de la taille des tables de routage
- Autres Lacunes de IPV4
  - Mobilité
  - Multicast
  - Sécurité
  - COS, QOS etc…

=> Nouvelle version du Protocole Internet : Version 6

ADRESSAGE IPv6

- Possibilités d'adressage étendues
  - de 32 bits à 128 bits
  - Préfixe réseau + Identifiant machine
- Format d'entête simplifié
  - traitement plus rapide
- Options intégrées dans des extensions d'entête

IPv6 : Les adresses

- Longueur 128 bits : 8 mots de 16 bits
  2001:0660:6101:0000:0000:0010:a123:0962
  Forme réduite ....
  2001:660:6101::10:a123:962

- Notion de préfixe hiérarchique.
  2000::/3 Global Unicast [RFC4291]
  2001:4200::/23 AfriNIC
  2001:4278::/32 SONATEL (Senegal)
  2001:4278:1000::/48 UCAD (Univ dakar)

IPv6 : Les adresses

- Ambiguité apparente de la notation
  - 2001:4278:1000:0000::/56
  - 2001:4278:1000::/56

  (Adresses Identiques)

  - 2001:4278:1000:0100::/56
  - 2001:4278:1000:100::/56

  (Adresses Identiques)

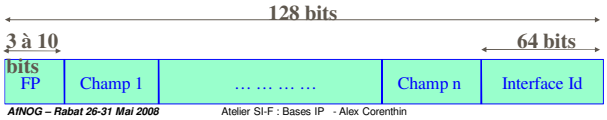
  (Préfixes identiques)
- Utilisation de ces adresses dans une URL
  - http://2001:4278:1000:100::1e/
  - http://[2001:4278:1000:100::1e]:8000/

IPv6 : Les adresses

- Trois types d'adresses
  - Unicast
    - Identifie une interface
  - Multicast
    - Indentifie un groupe d'interfaces
  - Anycast
    - Identifie une interface dans un groupe

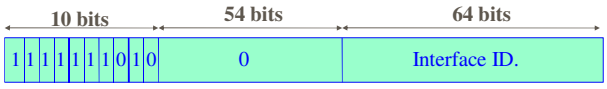
IPv6 : Les adresses
Adresses Unicast

- Adresse Unicast
  - Lien local *(FE80::/64)*
  - Site local *(FE0C::/64 n'est plus utilisé)*
  - Adresses unicast globales
  - Adresse de retour, loopback *(::1)*
  - Adresse indéterminée *(0:0:0:0:0:0:0:0)*



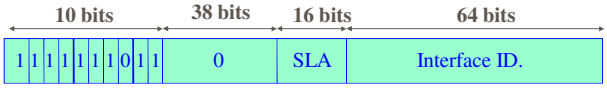
IPv6 : Les adresses
Adresses Unicast

- Lien Local
  - Le préfixe est de la forme : FE80::/64



IPv6 : Les adresses
Adresses Unicast

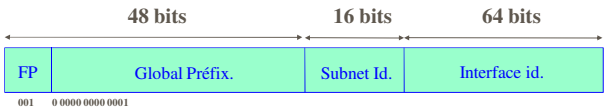
- Site Local (n'est plus utilisé: RFC 3879)
  - Le préfixe est de la forme : FEC0::/48
  - SLA 'Site Level Aggrégation' sur 16 bits



- Unique Local Address (RFC 4193)
  - Le préfixe est de la forme : FC00::/7

IPv6 : Les adresses
Adresses Unicast

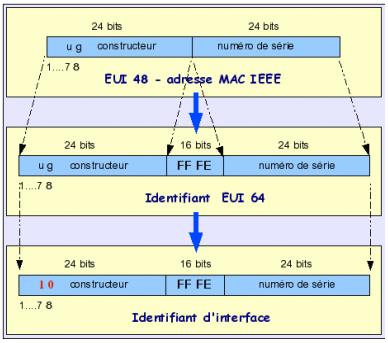
- Les adresses Unicast globales affectées aux organismes régionaux (R.I.R).
- Préfixe 2000::/3



IPv6 : Le protocole « mécanisme Plug & Play »

- Activation : par défaut dans FreeBSD
- Mécanisme de configuration automatique
  - Affectation de l'adresse lien-local et vérification de son unicité.
  - Découverte des routeurs présents sur le lien physique.
  - Découverte des préfixes du réseau.
  - Découverte des paramètres avancés.
- **Autoconfiguration Stateless**
  - Identifiant d'interface
    - Identifiant issu de l'adresse MAC EUI48 (RFC2464)

IPv6 : Identifiant EUI- 64



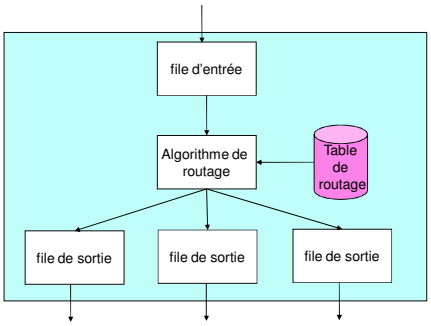
IPv6 : Autoconfiguration

- Autoconfiguration Stateless
  - Création de l'adresse unicast Lien local
    - fe80::xxxx:xxxx:xxxx:xxxx
    - Vérification de l'unicité : Sollicitation multicast des voisins ff02::1
  - Création de l'adresse unicast globale
    - Sollicitation multicast des routeurs ff02::2
    - Réponse contenant le prefixe 2001:660:6101:1::/64
    - Création de l'adresse globale 2001:4348:221:xxxx:xxxx:xxxx:xxxx

Concepts de l'interconnexion

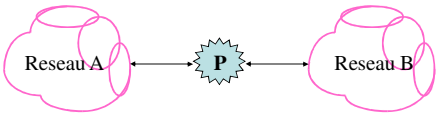
- Le concept d'interconnexion ou d'*internet* repose sur la mise en oeuvre d'une couche réseau masquant les détails de la communication physique du réseau et détachant les applications des problèmes de routage.
- L'interconnexion : faire transiter des informations depuis un réseau vers un autre réseau par des noeuds spécialisés appelés passerelles (*gateway*) ou routeurs (*router*)

Fonction Routeur



Concepts de l'interconnexion

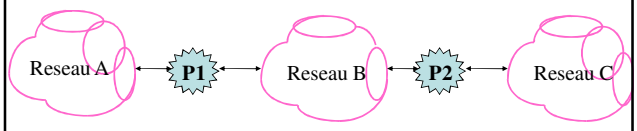
- Les routeurs possèdent une connexion sur chacun des réseaux:



La passerelle P interconnecte les réseaux A et B.

- Le rôle de la passerelle P est de transférer sur le réseau B, les paquets circulant sur le réseau A et destinés au réseau B et inversement.

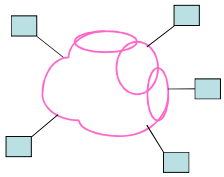
Concepts de l'interconnexion



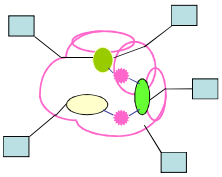
- P1 transfère sur le réseau B, les paquets circulant sur le réseau A et destinés aux réseaux B et C
- P1 doit avoir connaissance de la topologie du réseau; à savoir que C est accessible depuis le réseau B.
- Le routage n'est pas effectué sur la base de la machine destinataire mais sur la base du réseau destinataire

Concepts de l'interconnexion

- A l'intérieur de chaque réseau, les noeuds utilisent la technologie spécifique de leur réseau (Ethernet, X25, etc)
- Le logiciel d'interconnexion (couche réseau) encapsule ces spécificités et offre un service commun à tous les applicatifs, faisant apparaître l'ensemble de ces réseaux disparates comme un seul et unique réseau.



Vue utilisateur



Vue réelle du réseau